DEPARTMENT OF DEFENSE
PUBLICATION SYSTEM TRANSMITTAL

(2)

OFFICE OF THE SECRETARY OF DEFENSE
Assistant Secretary of Defense
for Command, Control, Communications,
and Intelligence

CHANGE NO. 2
DoD 5200.2-R
July 14, 1993

PERSONNEL SECURITY PROGRAM

The Assistant Secretary of Defense for Command, Control, Communications and Intelligence has authorized the following pen and page changes to DoD 5200.2-R, "Personnel Security Program," January 1987:

PEN CHANGES

Page ii, section 3
Delete "1-314 DoD National Agency Check Plus Written Inquiries (DNACI) ... I-4"
Renumber "1-315 through 1-327" to "1-314 through 1-326"

Page iii, section 3. Renumber "1-328 through 1-330" to "1-327 through 1-329"

Page vii, section 2. Change "VIII-3" to "VIII-4"

Page viii.. Delete "Appendix H - List of Designated Countries ... H-1"

Page I-5, renumber "1-319 through 1-325" to "1-318 through 1-324"

Page I-6, renumber "1-326 through 1-330" to "1-325 through 1-329"

Appendix E, page E-1, paragraph 3., line 2. Change "designated country (Appendix H)" to "foreign country or foreign intelligence service"

Appendix I, page I-13, Disqualifying Factors, paragraph 3., lines 3 and 4. Change "or in a country designated hostile to the United States (See Appendix H)" to "foreign intelligence services"

PAGE CHANGES

Remove: I-3&I-4, VI-3 through VIII-4, IX-3 through IX-5, X1-1&X1-2, B-11&B-12, and H-1

Insert: Attached replacement pages

WHEN PRESCRIBED ACTION HAS BEEN TAKEN, THIS TRANSMITTAL SHOULD BE FILED WITH THE BASIC DOCUMENT

NUMBER	DATE	DEPARTMENT OF DEFENSE
DoD 5200.2-R, Change 2	July 14, 1993	PUBLICATIONS SYSTEMS TRANSMITTAL

INSTRUCTIONS FOR RECIPIENTS (continued)

Changes appear on pages I-3&I-4, VI-3, VII-1&VII-2, VIII-2 through VIII-4, IX-3 through IX-5, X1-1&X1-2, and B-11&B-12 and are indicated by marginal asterisks.

EFFECTIVE DATE

These changes are effective immediately.

James L Elmer

JAMES L. ELMER
Director
Correspondence and Directives

Attachments: 17 pages

1-304 Defense Clearance and Investigative Index (DCII)

* The DCII is the single, automated, central DoD repository which identifies * investigations conducted by DoD investigative agencies, and personnel security * determinations made by DoD adjudicative authorities. *

1-305 DoD Component

* Includes the Office of the Secretary of Defense; the Military Departments; * Chairman of the Joint Chiefs of Staff and the Joint Staff; Directors of Defense Agencies and the Unified and Specified Commands.

1-306 Entrance National Agency Check (ENTNAC)

A personnel security investigation scoped and conducted in the same manner as a National Agency Check except that a technical fingerprint search of the files of the Federal Bureau of Investigation is not conducted.

1-307 Head of DoD Component

* The Secretary of Defense; the Secretaries of the Military Departments; the * Chairman of the Joint Chiefs of Staff; and the Commanders of Unified and Specified Commands; and the Directors of Defense Agencies.

1-308 Immigrant Alien

Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

1-309 Interim Security Clearance

A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

1-310 Limited Access Authorization

Authorization for access to Confidential or Secret information granted to non-United States citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years (paragraph 3, Appendix B).

1-311 Minor Derogatory Information

Information that, by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative action in a personnel security determination.

1-312 National Agency Check (NAC)

A personnel security investigation consisting of a records review of certain national agencies as prescribed in paragraph 1, Appendix B, this Regulation, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

1-313 National Agency Check Plus Written Inquiries (NACI)

A personnel security investigation conducted by the Office of Personnel Management, combining a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references and schools.

* 1-314 National Security *

National security means the national defense and foreign relations of the United States.

* 1-315 Need-to-know *

A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official United States Government program. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

* 1-316 Periodic Reinvestigation (PR) *

* An investigation conducted every five years for the purpose of updating a *
* previously completed background investigation, special background investigation, *
* single scope background investigation or PR on persons occupying positions referred *
* to in paragraphs 3-700 through 3-710. Investigative requirements are as prescribed *
* in paragraph 5, Appendix B, of this Regulation. The period of investigation will not *
* normally exceed the most recent 5-year period. *

* 1-317 Personnel Security Investigation (PSI) *

Any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the Department of Defense, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. PSIs include investigations of affiliations with subversive organizations, suitability information, or hostage situations (see paragraph

(1) The nature and seriousness of the conduct;

(2) The circumstances surrounding the conduct;

(3) The frequency and recency of the conduct;

(4) The age of the individual;

(5) The voluntariness of participation; and

(6) The absence or presence of rehabilitation.

b. Detailed adjudication policy guidance to assist adjudicators in determining whether a person is eligible for access to classified information or assignment to sensitive duties is contained in Appendix I. Adjudication policy for access to SCI is contained in DCID 1/14.

6-103 Adjudicative Record

* a. Each adjudicative determination, whether favorable or unfavorable, shall be entered into the Defense Clearance and Investigations Index (DCII) on a daily basis, but in no case to exceed 5 working days from the date of determination.

* b. The rationale underlying each unfavorable personnel security determination, to include the appeal process, and each favorable personnel security determination where the investigation or information upon which the determination was made included significant derogatory information of the type set forth in paragraph 2-200 and Appendix I of this Regulation, shall be maintained in written or automated form and is subject to the provisions of DoD Directives 5400.7 (reference (aa)) and 5400.11 (reference (bb)). This information shall be maintained for a minimum of 5 years from the date of determination.

CHAPTER VII

ISSUING CLEARANCE AND GRANTING ACCESS

7-100 General

a. The issuance of a personnel security clearance (as well as the function of determining that an individual is eligible for access to Special Access program information, or is suitable for assignment to sensitive duties or such other duties that require a trustworthiness determination) is a function distinct from that involving the granting of access to classified information. Clearance determinations are made on the merits of the individual case with respect to the subject's suitability for security clearance. Access determinations are made solely on the basis of the individual's need for access to classified information in order to perform official duties. Except for suspension of access pending final adjudication of a personnel security clearance, access may not be finally denied for cause without applying the provisions of paragraph 8-102.

b. Only the authorities designated in Paragraph A, Appendix F are authorized to grant, deny or revoke personnel security clearances or Special Access authorizations (other than SCI). Any commander or head of an organization may suspend access for cause when there exists information raising a serious question as to the individual's ability or intent to protect classified information, provided that the procedures set forth in paragraph 8-102 of this Regulation are complied with.

c. All commanders and heads of DoD organizations have the responsibility for determining those position functions in their jurisdiction that require access to classified information and the authority to grant access to incumbents of such positions who have been cleared under the provisions of this Regulation.

7-101 Issuing Clearance

a. Authorities designated in Paragraph A, Appendix F shall record the * issuance, denial, or revocation of a personnel security clearance in the DCII (see * paragraph 6-103, above). A record of the clearance issued shall also be recorded in an individual's personnel/security file or official personnel folder, as appropriate.

b. A personnel security clearance remains valid until (1) the individual is separated from the Armed Forces, (2) separated from DoD civilian employment, (3) has no further official relationship with DoD, (4) official action has been taken to deny, revoke or suspend the clearance or access, or (5) regular access to the level of classified information for which the individual holds a clearance is no longer necessary in the normal course of his or her duties. If an individual resumes the original status of (1), (2), (3), or (5) above, no single break in the individual's * relationship with DoD exists greater than 24 months, and/or the need for regular * access to classified information at or below the previous level recurs, the appropriate clearance shall be reissued without further investigation or adjudication provided there has been no additional investigation or development of derogatory information.

c. Personnel security clearances of DoD military personnel shall be granted, denied, or revoked only by the designated authority of the parent Military Department. Issuance, reissuance, denial, or revocation of a personnel security clearance by any DoD Component concerning personnel who have been determined to be eligible for clearance by another component is expressly prohibited. Investigations conducted on Army, Navy, and Air Force personnel by DIS will be returned only to the parent service of the subject for adjudication regardless of the source of the original request. The adjudicative authority will be responsible for expeditiously transmitting the results of the clearance determination. As an exception, the employing DoD Component may issue an interim clearance to personnel under their administrative jurisdiction pending a final eligibility determination by the individual's parent Component. Whenever an employing DoD component issues an interim clearance to an individual from another Component, written notice of the action shall be provided to the parent Component.

* d. When a Defense agency, to include the Chairman of the Joint Chiefs of Staff, initiates an SSBI (or PR) for access to SCI on a military member, DIS will return the completed investigation to the appropriate Military Department adjudicative authority in accordance with paragraph 7-101.c., above, for issuance (or reissuance) of the Top Secret clearance. Following the issuance of the security clearance, the military adjudicative authority will forward the investigative file to the Defense agency identified in the "Return Results To" block of the DD Form 1879. The receiving agency will then forward the completed SSBI to DIA for the SCI adjudication in accordance with DCID 1/14. *

e. The interim clearance shall be recorded in the DCSI (paragraph 6-103, above) by the parent DoD Component in the same manner as a final clearance.

7-102 Granting Access

a. Access to classified information shall be granted to persons whose official duties require such access and who have the appropriate personnel security clearance. Access determinations (other than for Special Access programs) are not an adjudicative function relating to an individual's suitability for such access. Rather they are decisions made by the commander that access is officially required.

b. In the absence of derogatory information on the individual concerned, DoD commanders and organizational managers shall accept a personnel security clearance determination, issued by any DoD authority authorized by this Regulation to issue personnel security clearance, as the basis for granting access, when access is required, without requesting additional investigation or investigative files.

* c. The access level of cleared individuals will, wherever possible, be entered into the Defense Clearance and Investigations Index (DCII), along with clearance eligibility. However, completion of the DCII Access field is required effective 1 October 1993 in all instances where the adjudicator is reasonably aware of the level of classified access associated with a personnel security investigation. Agencies are encouraged to start completing this field as soon as possible. *

7-103 Administrative Withdrawal

As set forth in paragraph 7-101.b., above, the personnel security clearance and access eligibility must be withdrawn when the events described therein occur. When regular access to a prescribed level of classified information is no longer

required in the normal course of an individual's duties, the previously authorized access eligibility level must be administratively downgraded or withdrawn, as appropriate.

#First Amendment (Ch 2, 7/14/93)

CHAPTER VIII

UNFAVORABLE ADMINISTRATIVE ACTIONS

Section I

REQUIREMENTS

8-100 General

For purposes of this Regulation, an unfavorable administrative action includes any adverse action which is taken as a result of a personnel security determination, as defined at paragraph 1-301, and any unfavorable personnel security determination, as defined at paragraph 1-329. This chapter is intended only to provide guidance for the internal operation of the Department of Defense and is not intended to, does not, and may not be relied upon, to create or enlarge the jurisdiction or review authority of any court or administrative tribunal, including the Merit Systems Protection Board.

8-101 Referral for Action

a. Whenever derogatory information related to the criteria and policy set forth in paragraph 2-2200 and Appendix I of this Regulation is developed or otherwise becomes available to any DoD element, it shall be referred by the most expeditious means to the commander or the security officer of the organization to which the individual is assigned for duty. The commander or security officer of the organization to which the subject of the information is assigned shall review the information in terms of its security significance and completeness. If further information is needed to confirm or disprove the allegations, additional investigation should be requested. The commander of the duty organization shall insure that the parent Component of the individual concerned is informed promptly concerning (1) the derogatory information developed and (2) any actions taken or anticipated with respect thereto. However, referral of derogatory information to the commander or security officer shall in no way affect or limit the responsibility of the central adjudication facility to continue to process the individual for denial or revocation of clearance or access to classified information, in accordance with paragraph 8-201, below, if such action is warranted and supportable by the criteria and policy contained in paragraph 2-200 and Appendix I. No unfavorable administrative action as defined in paragraph 1-328 and 329 may be taken by the organization to which the individual is assigned for duty without affording the person the full range of protections contained in paragraph 8-201, below, or, in the case of SCI, Annex B, DCID 1/14 (reference (l)).

b. The Director DIS shall establish appropriate alternative means whereby information with potentially serious security significance can be reported other than through DoD command or industrial organization channels. Such access shall include utilization of the DoD Inspector General "hotline" to receive such reports for appropriate follow-up by DIS. DoD Components and industry will assist DIS in publicizing the availability of appropriate reporting channels. Additionally, DoD Components will augment the system when and where necessary. Heads of DoD Components will be notified immediately to take action if appropriate.

8-102 Suspension

a. The commander or head of the organization shall determine whether, on the basis of all facts available upon receipt of the initial derogatory information, it is in the interests of national security to continue subject's security status unchanged or to take interim action to suspend subject's access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), if information exists which raises serious questions as to the individual's ability or intent to protect classified information or execute sensitive duties (or other duties requiring a trustworthiness determination) until a final determination is made by the appropriate authority designated in Appendix F.

b. Whenever a determination is made to suspend a security clearance for access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), the individual concerned must be notified of the determination in writing by the commander, or head of the component or adjudicative authority, to include a brief statement of the reason(s) for the suspension action consistent with the interests of national security.

c. Component field elements must promptly report all suspension actions to the appropriate central adjudicative authority, but not later than 10 working days from the date of the suspension action. The adjudicative authority will immediately update the DCII Eligibility and Access fields to alert all users to the individual's changed status.

d. Every effort shall be made to resolve suspension cases as expeditiously as circumstances permit. Suspension cases exceeding 180 days shall be closely monitored and managed by the DoD Component concerned until finally resolved. Suspension cases pending in excess of 12 months will be reported to the DASD (CI & SCM) for review and appropriate action.

e. A final security clearance eligibility determination shall be made for all suspension actions and the determination entered in the DCII. If, however, the individual under suspension leaves the jurisdiction of the Department of Defense and no longer requires a clearance (or trustworthiness determination), entry of the "Z" Code (adjudication action incomplete due to loss of jurisdiction) in the clearance eligibility field is appropriate. In no case shall a "suspension" code (Code Y) remain as a permanent record in the DCII.

f. A clearance or access entry in the DCII shall not be suspended or downgraded based solely on the fact that a periodic reinvestigation was not conducted precisely within the 5-year time period for TOP SECRET/SCI or within the period prevailing for SECRECT clearances under departmental policy. While every effort should be made to ensure that PRs are conducted within the prescribed timeframe, agencies must be flexible in their administration of this aspect of the personnel security program so as not to undermine the ability of the Department of Defense to accomplish its mission.

8-103 Final Unfavorable Administrative Actions

The authority to make personnel security determinations that will result in an unfavorable administrative action is limited to those authorities designated in Appendix F, except that the authority to terminate the employment of a civilian

employee of a military department or Defense agency is vested solely in the head of the DoD component concerned and in such other statutory official as may be designated. Action to terminate civilian employees of the Office of the Secretary of Defense and DoD Components, on the basis of criteria listed in paragraph 2-200, a through f, shall be coordinated with the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence OASD (C3I) prior to final action by the head of the DoD Component. DoD civilian employees or members of the Armed Forces shall not be removed from employment or separated from the Service under provisions of this regulation if removal or separation can be effected under OPM regulations or administrative (nonsecurity) regulations of the military departments. However, actions contemplated in this regard shall not affect or limit the responsibility of the central adjudication facility to continue to process the individual for denial or revocation of a security clearance, access to classified information, or assignment to a sensitive position if warranted and supportable by the criteria and standards contained in this Regulation.

Section 2

PROCEDURES

8-200 General

No final personnel security determination shall be made on a member of the Armed Forces, an employee of the Department of Defense, a consultant to the Department of Defense, or any other person affiliated with the Department of Defense without granting the individual concerned the procedural benefits set forth in 8-201 below, when such determination results in an unfavorable administrative action (see paragraph 8-100). As an exception, Red Cross/United Service Organizations employees shall be afforded the procedures prescribed by DoD Directive 5210.25 (reference (w)).

8-201 Unfavorable Administrative Action Procedures

Except as provided for below, no unfavorable administrative action shall be taken under the authority of this Regulation unless the person concerned has been given:

a. A written statement of the reasons why the unfavorable administrative action is being taken. The statement shall be as comprehensive and detailed as the protection of sources afforded confidentiality under provisions of the Privacy Act of 1974 (5 U.S.C. 522a) (reference (m)) and national security permit. The statement will also provide the name and address of the agency (agencies) to which the individual may write to obtain a copy of the investigative file(s) upon which the unfavorable administrative action is being taken. Prior to issuing a statement of reasons to a civilian employee for suspension or removal action, the issuing authority must comply with the provisions of Federal Personnel Manual, Chapter 732, Subchapter 1, paragraph 1-6b (reference (cc)). The signature authority must be as provided for in paragraph 6-101.b.(1)(b) and 6-101.b.(2)(b).

b. An opportunity to reply in writing to such authority as the head of the Component concerned may designate.

c. A written response to any submission under subparagraph b. stating the final reason therefor, which shall be as specific as privacy and national security considerations permit. The signature authority must be as provided for in paragraphs 6-101.b.(1)(b) and 6-101.b.(2)(b). Such response shall be as prompt as individual circumstances permit, not to exceed 60 days from the date of receipt of the appeal submitted under subparagraph b., above, provided no additional investigative action is necessary. If a final response cannot be completed within the time frame allowed, the subject must be notified in writing of this fact, the reasons therefor, and the date a final response is expected, which shall not, in any case, exceed a total of 90 days from the date of receipt of the appeal under subparagraph b.

d. An opportunity to appeal to a higher level of authority designated by the Component concerned.

8-202 Exceptions to Policy

Not withstanding paragraph 8-201 above or any other provision of this Regulation, nothing in this Regulation shall be deemed to limit or affect the responsibility and powers of the Secretary of Defense to find that a person is unsuitable for entrance or retention in the Armed Forces, or is ineligible for a security clearance or assignment to sensitive duties, if the national security so requires, pursuant to Section 7532, Title 5, United States Code (reference (pp)). Such authority may not be delegated and may be exercised only when it is determined that the procedures prescribed in paragraph 8-201 above are not appropriate. Such determination shall be conclusive.

Section 3

REINSTATEMENT OF CIVILIAN EMPLOYEES

8-300 General

Any person whose civilian employment in the Department of Defense is terminated under the provisions of this Regulation shall not be reinstated or restored to duty or reemployed in the Department of Defense unless the Secretary of Defense, or the head of a DoD Component, finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of national security. Such a finding shall be made part of the personnel security record.

8-301 Reinstatement Benefits

A DoD civilian employee whose employment has been suspended or terminated under the provisions of this Regulation and who is reinstated or restored to duty under the provisions of Section 3571 of Title 5, U.S. Code (reference (dd)) is entitled to benefits as provided for by Section 3 of Public Law 89-380 (reference (ee)).

b. Moreover, individuals having access to classified information must report promptly to their security office:

* (1) Any form of contact, intentional or otherwise, with individuals of any nationality, whether within or outside the scope of the employee's official activities, in which:

* (a) Illegal or unauthorized access is sought to classified or otherwise sensitive information.

* (b) The employee is concerned that he or she may be the target of exploitation by a foreign entity.

(2) Any information of the type referred to in paragraph 2-200 or Appendix I.

9-104 Co-worker Responsibility

Co-workers have an equal obligation to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified information employed in a sensitive position.

Section 2

SECURITY EDUCATION

9-200 General

The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them. Thus, an integral part of the DoD security program is the indoctrination of individuals on their security responsibilities. Moreover, such indoctrination is essential to the efficient functioning of the DoD personnel security program. Accordingly, heads of DoD Components shall establish procedures in accordance with this chapter whereby persons requiring access to classified information, or being assigned to positions that require the occupants to be determined trustworthy are periodically briefed as to their security responsibilities.

9-201 Initial Briefings

a. All persons cleared for access to classified information or assigned to duties requiring a trustworthiness determination under this Regulation shall be given an initial security briefing. The briefing shall be in accordance with the requirements of paragraph 10-102, DoD 5200.1-R (reference (q)) and consist of the following elements:

(1) The specific security requirements of their particular job.

(2) The techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility for reporting such attempts.

(3) The prohibition against disclosing classified information, by any means, to unauthorized persons or discussing or handling classified information in a manner that would make it accessible to unauthorized persons.

(4) The penalties that may be imposed for security violations.

* b. If an individual declines to execute Standard Form 312, "Classified * Information Nondisclosure Agreement" (replaced the Standard Form 189), the DoD * Component shall initiate action to deny or revoke the security clearance of such * person in accordance with paragraph 8-102, above.

9-202 Refresher Briefing

Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information. The elements outlined in paragraph 10-101, DoD 5200.1-R (reference (q)) shall be tailored to fit the needs of the experienced personnel.

9-203 Foreign Travel Briefing

* While world events during the past several years have diminished the threat to our national security from traditional cold-war era foreign intelligence services, foreign intelligence services continue to pursue the unauthorized acquisition of classified or otherwise sensitive U.S. Government information, through the recruitment of U.S. Government employees with access to such information. Through security briefings and education, the Department of Defense continues to provide for the protection of information and technology considered vital to the national security interests from illegal or unauthorized acquisition by foreign intelligence services.

a. DoD Components will establish appropriate internal procedures requiring all personnel possessing a DoD security clearance to report to their security office all contacts with individuals of any nationality, whether within or outside the scope of the employee's official activities, in which:

(1) Illegal or unauthorized access is sought to classified or otherwise sensitive information.

(2) The employee is concerned that he or she may be the target of exploitation by a foreign entity.

b. The DoD security manager, security specialist, or other qualified individual will review and evaluate the reported information. Any facts or circumstances of a reported contact with a foreign national that appear to:

(1) Indicate an attempt or intention to obtain unauthorized access to proprietary, sensitive, or classified information or technology,

(2) Offer a reasonable potential for such, or

(3) Indicate the possibility of continued contact with the foreign national for such purposes,

shall be promptly reported to the appropriate counterintelligence agency. *

9-204 Termination Briefing

a. Upon termination of employment administrative withdrawal of security clearance, or contemplated absence from duty or employment for 60 days or more, DoD military personnel and civilian employees shall be given a termination briefing, return all classified material, and execute a Security Termination Statement. This statement shall include:

(1) An acknowledgment that the individual has read the appropriate provisions of the Espionage Act, other criminal statutes, DoD Regulations applicable to the safeguarding of classified information to which the individual has had access, and understands the implications thereof;

(2) A declaration that the individual no longer has any documents or material containing classified information in his or her possession;

(3) An acknowledgment that the individual will not communicate or transmit classified information to any unauthorized person or agency; and

(4) An acknowledgment that the individual will report without delay to the FBI or DoD Component concerned any attempt by any unauthorized person to solicit classified information.

b. When an individual refuses to execute a Security Termination Statement, that fact shall be reported immediately to the security manager of the cognizant organization concerned. In any such case, the individual involved shall be debriefed orally. * The fact of a refusal to sign a Security Termination Statement shall be reported to the Director, Defense Investigative Service, who shall ensure that it is recorded in the Defense Clearance and Investigations Index. *

c. The Security Termination Statement shall be retained by the DoD Component that authorized the individual access to classified information for the period specified in the Component's records retention schedules, but for a minimum of 2 years after the individual is given a termination briefing.

d. In addition to the provisions of subparagraphs a., b., and c. above, DoD Components shall establish a central authority to be responsible for ensuring that Security Termination Statements are executed by senior personnel (general officers, flag officers and GS-16s and above). Failure on the part of such personnel to execute a Security Termination Statement shall be reported immediately to the Deputy Under Secretary of Defense for Policy.

CHAPTER XI

PROGRAM MANAGEMENT

11-100 General

To ensure uniform implementation of the DoD personnel security program throughout the Department, program responsibility shall be centralized at the DoD Component level.

11-101 Responsibilities

* a. The Assistant Secretary of Defense for Command, Control, Communications * and Intelligence (ASD(C3I)) shall have primary responsibility for providing guidance, oversight, development and approval for policy and procedures governing personnel security program matters within the Department:

(1) Provide program management through issuance of policy and operating guidance.

(2) Provide staff assistance to the DoD Components and defense agencies in resolving day-to-day security policy and operating problems.

(3) Conduct inspections of the DoD Components for implementation and compliance with DoD security policy and operating procedures.

(4) Provide policy, oversight, and guidance to the component adjudication functions.

(5) Approve, coordinate and oversee all DoD personnel security research initiatives and activities.

b. The General Counsel shall ensure that the program is administered in a manner consistent with the laws; all proceedings are promptly initiated and expeditiously completed; and that the rights of individuals involved are protected, consistent with the interests of national security. The General Counsel shall also ensure that all relevant decisions of the courts and legislative initiatives of the Congress are obtained on a continuing basis and that analysis of the foregoing is accomplished and disseminated to DoD personnel security program management authorities.

c. The Heads of the Components shall ensure that:

(1) The DoD personnel security program is administered within their area of responsibility in a manner consistent with this Regulation.

(2) A single authority within the office of the head of the DoD Component is assigned responsibility for administering the program within the Component.

* (3) Information and recommendations are provided the ASD (C3I) and the * * General Counsel at their request concerning any aspect of the program. *

#First Amendment (Ch 2, 7/14/93)

11-102 Reporting Requirements

a. The OASD (C3I) shall be provided personnel security program management data by the Defense Data Manpower Center (DMDC) by 31 December each year for the preceding fiscal year. To facilitate accurate preparation of this report, all adjudicative determinations must be entered into the DCII by all DoD central adjudication facilities no later than the end of the fiscal year. The information required below is essential for basic personnel security program management and in responding to requests from the Secretary of Defense and Congress. The report shall cover the preceding fiscal year, broken out by clearance category, according to military (officer or enlisted), civilian or contractor status and by the central adjudication facility that took the action, using the enclosed format:

(1) Number of Top Secret, Secret and Confidential clearances issued;

(2) Number of Top Secret, Secret and Confidential clearances denied

(3) Number of Top Secret, Secret and Confidential clearances revoked;

(4) Number of SCI access determinations issued;

(5) Number of SCI access determinations denied;

(6) Number of SCI access determinations revoked; and

(7) Total number of personnel holding a clearance for Top Secret, Secret, Confidential and Sensitive Compartmented Information as of the end of the fiscal year.

b. The Defense Investigative Service (DIS) shall provide the OASD (C3I) a quarterly report that reflects investigative cases opened and closed during the most recent quarter, by case category type, and by major requester. The information provided by DIS is essential for evaluating statistical data regarding investigative workload and the manpower required to perform personnel security investigations. Case category types include National Agency Checks (NACs); Expanded NACs; Single Scope Background Investigations; Periodic Reinvestigations (PRs); SECRET Periodic Reinvestigations (SPRs); Post Adjudicative; Special Investigative Inquiries (SIIs); and Limited Inquiries. This report shall be forwarded to OASD (C3I) within 45 days after the end of each quarter.

c. The reporting requirement for DMDC and DIS has been assigned Report Control Symbol DD-C3I(A) 1749.

11-103 Inspections

The heads of DoD Components shall assure that personnel security program matters are included in their administrative inspection programs.

#First Amendment (Ch 2, 7/14/93)

be limited to that necessary to bring the individual's file up to date in accordance with the investigative requirements of an SBI. Should new information be developed during the current investigation that bears unfavorably upon the individual's activities covered by the previous investigation, the current inquiries shall be expanded as necessary to develop full details of this new information.

5. Periodic Reinvestigation (PR)

a. Each DoD military, civilian, consultant, and contractor employee (to include non - U.S. citizens (foreign nationals and/or immigrant aliens) holding a limited access authorization)) occupying a critical sensitive position, possessing a TOP SECRET clearance, or occupying a special access program position shall be the subject of a PR initiated 5 years from the date of completion of the last investigation. The PR shall cover the period of the last 5 years. *

b. Minimum Investigative Requirements. A PR shall include the following minimum scope.

(1) NAC. A valid NAC on the SUBJECT will be conducted in all cases. Additionally, for positions requiring SCI access, checks of DCII, FBI/HQ, FBI/ID name check only, and other agencies deemed appropriate, will be conducted on the SUBJECT's current spouse or cohabitant, if not previously conducted. Additionally, NACs will be conducted on immediate family members, 18 years of age or older, who are aliens and/or immigrant aliens, if not previously accomplished.

(2) Credit. Credit bureau checks covering all places where the SUBJECT resided for 6 months or more, on a cumulative basis, during the period of investigation, in the 50 states, District of Columbia, Puerto Rico and overseas (where APO/FPO addresses are provided), will be conducted.

(3) Subject Interview. The interview should cover the entire period of time since the last investigation, not just the last 5-year period. Significant information disclosed during the interview, which has been satisfactorily covered during a previous investigation, need not be explored again unless additional relevant information warrants further coverage. An SI is not required if one of the following conditions exist:

(a) The SUBJECT is aboard a deployed ship or in some remote area that would cause the interview to be excessively delayed.

(b) The SUBJECT is in an overseas location serviced by the State Department or the FBI.

(4) Employment. Current employment will be verified. Military and federal service records will not routinely be checked, if previously checked by the requester when the PR was originally submitted. Also, employment records will be checked wherever employment interviews are conducted. Records need be checked only when they are locally available, unless unfavorable information had been detected.

(5) Employment References. Two supervisors or co-workers at the most recent place of employment or duty station of 6 months; if the current employment is less than 6 months employment reference interviews will be conducted at the next prior place of employment, which was at least a 6-month duration.

(6) Developed Character References (DCRs). Two developed character references who are knowledgeable of the SUBJECT will be interviewed. Developed character references who were previously interviewed will only be reinterviewed when other developed references are not available.

(7) Local Agency Checks (LACs). DIS will conduct local agency checks on the SUBJECT at all places of residence, employment, and education during the period of investigation, regardless of duration, including overseas locations.

* (8) Neighborhood Investigation. Conduct a neighborhood investigation to verify subject's current residence in the United States. Two neighbors who can verify subject's period of residence in that area and who are sufficiently acquainted to comment on the subject's suitability for a position of trust will be interviewed. Neighborhood investigations will be expanded beyond the current residence when unfavorable information arises. *

* (9) Ex-spouse Interview. If the subject of investigation is divorced, the ex-spouse will be interviewed when the date of final divorce action is within the period of investigation. *

* (10) Select Scoping. When the facts of the case warrant, additional select scoping will be accomplished, as necessary, to fully develop or resolve an issue. *

#First Amendment Ch 2, 7/14/93)